UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OKLAHOMA

KATHY DEEVERS, individually and on behalf of all others similarly situated, Plaintiff, v. WING FINANCIAL SERVICES LLC, Defendant.	**Case No. 4:22-CV-00550-CVE-JFJ** **CLASS ACTION** **CONSOLIDATED CLASS ACTION COMPLAINT** **[JURY TRIAL DEMANDED]**
VENELIN STOICHEV, individually, and on behalf of all others similarly situated, Plaintiff, v. WING FINANCIAL SERVICES, LLC., Defendant.	

Representative Plaintiffs on behalf of themselves and all others similarly situated, bring this Consolidated Amended Class Action Complaint against Defendant Wing Financial Services LLC ("Defendant") and make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

INTRODUCTION

1. Representative Plaintiffs Kathy Deevers and Venelin Stoichev ("Representative Plaintiffs") bring this class action against Defendant Wing Financial Services, LLC ("Defendant" or "Wing") for its failure to properly secure and safeguard Representative Plaintiffs' and Class Members' personally identifiable information stored within Defendant's information network, including, without limitation, their financial account numbers and access codes, credit card

numbers and security codes. (These types of information, *inter alia*, being thereafter referred to, collectively, as "personally identifiable information" or "PII").[1]

2. Wing is an independently owned and operated Jackson Hewitt franchise that provides tax preparation services on behalf of individuals. Clients are required to provide their sensitive personal information, including non-public financial information, to Wing as a condition of doing business.

3. With this action, Representative Plaintiffs seek to hold Wing responsible for the harms it caused and will continue to cause Representative Plaintiffs and approximately 243,403[2] other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendant on or around August 7, 2022, by which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PII was being insufficiently protected (the "Data Breach").

4. Representative Plaintiffs further seek to hold Wing responsible for not ensuring that the PII was maintained in a manner consistent with industry and other relevant standards.

5. While Wing claims to have discovered the breach as early as August 7, 2022, it did not begin informing victims of the Data Breach until December 1, 2022, and failed to inform victims when or for how long the Data Breach occurred. Indeed, Representative Plaintiffs and Class Members were wholly unaware of the Data Breach until they received letters from Defendant

---

[1] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[2] *https://apps.web.maine.gov/online/aeviewer/ME/40/66a83c31-d1a0-462c-9025-e41c8344d707.shtml* (last accessed March 8, 2023).

informing them of it. The notice received by Representative Plaintiffs was dated December 1, 2022.

6. Wing's notice reported that the scope of information involved included: name, Social Security number, medical data, insurance information, government identification, state identification, driver's license number, financial account number and access code, tax identification number, address, biometric information, birthday, health insurance and policy information, and payment card number.

7. By obtaining, collecting, using, and deriving a benefit from Representative Plaintiffs' and Class Members' PII and PHI, Wing assumed legal and equitable duties to those individuals. These duties arise from state and federal statutes and regulations as well as common law principles.

8. Wing disregarded the rights of Representative Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiffs' and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Representative Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Representative Plaintiffs and Class Members in the future. Representative Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

9. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member is a citizen of a state different from Defendant.

10. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

11. Defendant conducts business in the State where this district is located, has sufficient minimum contacts in this State, and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

12. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Representative Plaintiffs' claims took place within this District, and Wing does business in this Judicial District.

PARTIES

PLAINTIFFS

Plaintiff Venelin Stoichev's Experience

13. Plaintiff Venelin Stoichev is an adult individual and, at all relevant times herein was and is a citizen of Oklahoma, who resides in Oklahoma City, Oklahoma.

14. Wing Financial received highly sensitive personal and financial information from Plaintiff Venelin Stoichev. As a result, Plaintiff Venelin Stoichev's information was among the data accessed by an unauthorized third-party in the Data Breach.

15. Representative Plaintiffs received—and were "consumers" for purposes of obtaining services from Defendant within this State.

16. At all relevant times herein, Plaintiff Venelin Stoichev, is and was, a member of each of the Class(es)/Subclass(es).

17. Plaintiff Venelin Stoichev provided Defendant with highly sensitive personal and financial information.

18. Plaintiff Venelin Stoichev's PII was exposed in the Data Breach because Defendant stored and/or shared Representative Plaintiffs' PII. His PII was within the possession and control of Defendant at the time of the Data Breach.

19. Plaintiff Venelin Stoichev received a letter from Defendant, dated December 1, 2022, stating that his PII was involved in the Data Breach (the "Notice").

20. As a result, Plaintiff Venelin Stoichev spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring his accounts and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

21. Plaintiff Venelin Stoichev suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant—which was compromised in and as a result of the Data Breach.

22. Plaintiff Venelin Stoichev suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has fear and anxiety and increased concerns for the loss of privacy, as well as fear and anxiety over the impact of cybercriminals accessing, using, and selling his PII.

23. In addition, he was notified in December of 2022 by Best Buy that a person in another state (where he has had no dealings) attempted to make a purchase using his Best Buy Visa card. Fortunately, Best Buy contacted Mr. Stoichev before approving the purchase and related credit increase. This clearly indicates that his information has been sold on the dark web and bad actors are already attempting to use it. In addition, Mr. Stoichev has no way to know if other attempts to use his personal information have been successful.

24. Plaintiff Stoichev has received multiple phone calls from loan companies asking for information about loan applications that he never submitted. He has also seen a marked increase in spam phone calls to his cell phone.

25. Plaintiff Venelin Stoichev has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

26. Plaintiff Venelin Stoichev has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Kathy Deevers' Experience

27. Plaintiff Kathy Deevers is an adult individual at all relevant times herein is and was a citizen of the State of Oklahoma who resides in Duncan, Oklahoma. Plaintiff Kathy Deevers previously received tax preparation services from Defendant and is one of its customers.

28. On December 1, 2022, Plaintiff Kathy Deevers was notified by Wing Financial via letter of the Data Breach and of the impact to her PII.

29. As a result of Defendant's conduct, Plaintiff Kathy Deevers suffered actual damages including, without limitation, time and expenses related to monitoring her financial

accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, fear and anxiety due to the increased risk, the lost value of her personal information, and other economic and non-economic harm. Plaintiff Kathy Deevers and Class Members will now be forced to expend additional time to review their credit reports and monitor their financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

30. Defendant Wing Financial is a financial services company with its principal place of business and headquarters at 2301 SE Washington Blvd, Bartlesville, OK 74006.

DEFENDANT

31. Defendant is an Oklahoma corporation with a principal place of business located at 2301 SE Washington Blvd, Bartlesville, OK 74006, USA. Defendant provides investment advice.[3]

32. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiffs. Representative Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such his responsible parties when those identities become known.

[3] https://www.dnb.com/business-directory/company-profiles.wing_financial_services_llc.7f38d66cec99501acc3848f2941d28bc.html (last accessed March 8, 2023).

COMMON FACTUAL ALLEGATIONS

A. Defendant Collected/Stored Class Members' PII and Financial Information as a Condition of its Business and Should Have Reasonably Anticipated the Data Breach

33. Representative Plaintiffs and the proposed Class are clients of Wing. Wing is a financial services company and is an independently owned and operated franchise of Jackson Hewitt, a tax-preparation service.

34. As a condition of providing financial services, Defendant acquired, collected and stored and assured reasonable security over Representative Plaintiffs' and Class Members' PII and financial information.

35. As a condition of its relationships with Representative Plaintiffs and Class Members, Defendant required that Representative Plaintiffs and Class Members entrust Defendant with highly sensitive and confidential PII and financial information. Defendant, in turn, stored that information of Defendant's system that was ultimately affected by the Data Breach.

36. By obtaining, collecting, and storing Representative Plaintiffs' and Class Members' PII and financial information, Defendant assumed legal and equitable duties and knew or should have known that they were thereafter responsible for protecting Representative Plaintiffs' and Class Members' PII and financial information from unauthorized disclosure.

37. Because of the highly sensitive and personal nature of the information Wing acquires and stores with respect to its clients, Wing, upon information and belief, promises to, among other things: keep clients' and customers' PII private; comply with industry standards related to data security and PII; inform customers and clients of legal duties and comply with all federal and state laws protecting customers' and clients' PII; only use and release PII for reasons

that relate to the financial services it is contracted to provide; and provide adequate notice to customers and clients if their PII is disclosed without authorization.

38. Representative Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and financial information. Representative Plaintiffs and Class Members relied on Defendant to keep their PII and financial information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

39. Defendant could have prevented the Data Breach, which began no later than September of 2020, by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Representative Plaintiffs' and Class Members' PII and financial information.

40. Defendant's negligence in safeguarding Representative Plaintiffs' and Class Members' PII and financial information is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

41. For example, Universal Health Services experienced a cyberattack on September 29, 2020 that appears similar to the attack on Defendant. As a result of this attack, Universal Health Services suffered a four-week outage of its systems which caused as much as $67 million in recovery costs and lost revenue.[4] Similarly, in 2021, Scripps Health suffered a cyberattack, an event which effectively shut down critical health care services for a month and left numerous

[4] https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-2020-fourth-quarter-and (last accessed November 5, 2021).

patients unable to speak to their physicians or access vital medical and prescription records.[5] A few months later, University of San Diego Health suffered a similar attack.[6]

42. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operation with the resources to put adequate data security protocols in place.

43. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Representative Plaintiffs' and Class Members' PII and financial information from being compromised.

44. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3rd Cir. 2015).

45. In addition to its obligations under federal and state laws, Defendant owed a duty to Representative Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII and financial information in Defendant's possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. Defendant owed a duty to Representative Plaintiffs and Class Members to provide reasonable

[5] https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-internal-systems-hit-by-cyberattack-2/2619540/ (last accessed March 8, 2023).
[6] https://www.nbcsandiego.com/news/local/data-breach-at-uc-san-diego-health-some-employee-email-accounts-impacted/2670302/ (last accessed March 8, 2023).

security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII and financial information of Representative Plaintiffs and Class Members.

46. Defendant owed a duty to Representative Plaintiffs and Class Members to design, maintain, and test its computer systems, servers and networks to ensure that the PII and financial information in its possession was adequately secured and protected.

47. Defendant owed a duty to Representative Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII and financial information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

48. Defendant owed a duty to Representative Plaintiffs and Class Members to implement processes that would immediately detect a breach on its data security systems in a timely manner.

49. Defendant owed a duty to Representative Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

50. Defendant owed a duty to Representative Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII and/or financial information from theft because such an inadequacy would be a material fact in the decision to entrust this PII and/or financial information to Defendant.

51. Defendant owed a duty of care to Representative Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

52. Defendant owed a duty to Representative Plaintiffs and Class Members to encrypt and/or more reliably encrypt Representative Plaintiffs' and Class Members' PII and financial information and monitor user behavior and activity in order to identity possible threats.

B. The Cyberattack

53. In the course of the Data Breach, one or more unauthorized third parties accessed Plaintiffs' and Class Members' sensitive data including, but not limited to, dates of birth, driver's license numbers, and Social Security numbers. Representative Plaintiffs were among the individuals whose data was accessed in the Data Breach.

54. According to the Data Breach Notification, which Defendant filed with the Office of the Maine Attorney General among other state Attorneys General, 243,403 persons were originally reported affected by the Data Breach.[7]

55. Representative Plaintiffs were provided the information detailed above upon receipt of a letter from Defendant, dated December 1, 2022. Representative Plaintiffs were not aware of the Data Breach—or even that Defendant was still in possession of their data until receiving that letter.

C. Defendant's Failed Response to the Breach

56. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiffs' and Class Members' PII and financial information with the intent of engaging in misuse of the PII and financial information, including marketing and selling Representative Plaintiffs' and Class Members' PII.

[7] Breach Portal, https://apps.web.maine.gov/online/aeviewer/ME/40/266008e2-e657-41cb-a258-40357b43c24b.shtml (last accessed March 8, 2023).

57. Not until roughly four months after it claims to have discovered the Data Breach did Defendant begin sending the Notice to persons whose PII and/or financial information Defendant confirmed was potentially compromised as a result of the Data Breach. The Notice provided basic details of the Data Breach and Defendant's recommended next steps.

58. The Notice included, *inter alia*, the claims that Defendant had learned of the Data Breach on August 7, 2022, and later discovered the unauthorized access began as early as September 2020.

59. Defendant's Notice provided scant detail, particularly considering the size and scope of the Data Breach and the sensitivity of Representative Plaintiffs' and Class Members' compromised information. The Notice states, in relevant part, that "certain client records were accessible to unauthorized parties on the internet" and that Defendant's investigation "determined that there had been unauthorized access to Wing Financial's systems."[8] The Notice went on to describe the information that was potentially compromised in the Data Breach, including names, addresses, dates of birth, unique biometric information, Social Security numbers, driver's license numbers or other state identification card numbers, individual tax identification numbers, passport numbers or other government ID, tax identification numbers, financial account numbers with access codes, payment card numbers, health insurance policy numbers, and medical treatment/history.

60. Defendant's Notice did not disclose how it discovered the cybersecurity incident, the means and mechanisms of the cybersecurity attack, the reason for its nearly four-month delay in notifying Representative Plaintiffs and the Class of the Data Breach, how it determined that

[8] https://apps.web.maine.gov/online/aeviewer/ME/40/266008e2-e657-41cb-a258-40357b43c24b/2490b09b-a603-43d6-843f-38711c393ab0/document.html

client records were "accessible", and what exact steps it took following the Data Breach to secure its systems and prevent future cyberattacks.

61. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiffs' and Class Members' PII and financial information, and medical history with the intent of engaging in misuse of the PII, financial information, and medical information, including marketing and selling Representative Plaintiffs' and Class Members' PII.

62. Defendant had and continues to have obligations created by applicable federal and state law as set forth herein, reasonable industry standards, common law, and its own assurances and representations to keep Representative Plaintiffs' and Class Members' PII confidential and to protect such PII from unauthorized access.

63. Representative Plaintiffs and Class Members were required to provide their PII and financial information to Defendant, which created, collected, and stored Representative Plaintiffs' and Class Members' PII with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

64. Despite this, Representative Plaintiffs and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used, and what steps are being taken, if any, to secure their PII going forward. Representative Plaintiffs and Class Members are, thus, left to speculate as to where their PII ended up, who has used it and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

65. Representative Plaintiffs' and Class Members' PII may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and financial information for targeted marketing without the approval of Representative Plaintiffs and/or Class Members. Either way, unauthorized individuals can now easily access the PII of Representative Plaintiffs and Class Members.

D. Defendant Was Obligated To Safeguard The Private Information Under HIPAA And Its Conduct Violated HIPAA

67. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[9]

68. HIPAA provides specific privacy rules that require covered entities to implement comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII is properly maintained.[10]

69. Defendant is a HIPAA covered business associate who electronically transmits and/or maintains personal health information ("PHI") in connection with its business transactions. As a regular and necessary part of its business, Defendant collects and custodies the highly sensitive Private Information of its clients', including, upon information and belief, health insurance and policy information and medical data. Defendant is required under federal and state

[9] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[10] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

law to maintain the strictest confidentiality of the patient's Private Information that it requires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

70. As a HIPAA covered entity, Defendant is required to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

71. By obtaining, collecting, using, and deriving a benefit from Representative Plaintiffs and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Representative Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

72. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains, and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding

individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

73. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

74. The high value of PII, PHI, and financial information to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[12] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[13]

75. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiffs and Class Members. For example, it is believed that certain PII was compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

76. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

---

[11] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 28, 2021).

[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed March 8, 2023).

[13] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed March 8, 2023).

77. Identity thieves can use PII, PHI, and financial information, such as that of Representative Plaintiffs and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

78. The ramifications of Defendant's failure to keep secure Representative Plaintiffs' and Class Members' PII, PHI, and financial information are long lasting and severe. Once PII, PHI, and financial information is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PII, PHI, and/or financial information of Representative Plaintiffs and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII, PHI, and/or financial information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

79. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[14]

[14] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed March 8, 2023).

80. When cyber criminals access financial information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Representative Plaintiffs and Class Members.

81. And data breaches are preventable.[15] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[16] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[17]

82. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[18]

83. Here, Defendant knew of the importance of safeguarding PII, PHI and financial information and of the foreseeable consequences that would occur if Representative Plaintiffs' and Class Members' PII, PHI, and financial information was stolen, including the significant costs that would be placed on Representative Plaintiffs and Class Members as a result of a breach of this magnitude. As detailed above, Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. They knew, or should have known, that the development

[15] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)
[16] *Id.* at 17.
[17] *Id.* at 28.
[18] *Id.*

and use of such protocols were necessary to fulfill its statutory and common law duties to Representative Plaintiffs and Class Members. Its failure to do so is, therefore, intentional, willful, reckless and/or grossly negligent.

84. Defendant disregarded the rights of Representative Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiffs' and Class Members' PII, PHI, and/or financial information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Representative Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

85. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Representative Plaintiffs' and Class Members' confidential PII and PHI.

86. However, due to Defendant's failures, Representative Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Representative Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendant.

87. Representative Plaintiffs and Class Members have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

b. Trespass, damage to, and theft of their personal property, including PII and PHI;

c. Improper disclosure of their PII and PHI;

d. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII being in the hands of criminals and having already been misused;

e. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

f. Fear and anxiety over the imminent and impending risks of of ther PII and PHI being in the hands of criminals.

g. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

h. Loss of privacy suffered as a result of the Data Breach;

i. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

j. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

k. The loss of use of and access to their credit, accounts, and/or funds;

l. Damage to their credit due to fraudulent use of their Private Information; and

m. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

88. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII and PHI, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiffs' and Class Members' PII and PHI.

89. Plaintiffs and Class Members also have an interest in ensuring that their personal information that was provided to Defendant is removed from Defendant's unencrypted files.

CLASS ACTION ALLEGATIONS

90. Representative Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and the following classes/subclass(es) (collectively, the "Class"):

> **Nationwide Class:**
> "All individuals within the United States of America whose PII, PHI, and/or financial information was exposed to unauthorized third-parties as a result of the data breach discovered by Defendant on August 9, 2022."

> **Oklahoma Subclass:**
> "All individuals within the State of Oklahoma whose PII, PHI, was stored by Defendant and/or was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on August 9, 2022."

91. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

92. Also, in the alternative, Representative Plaintiffs requests additional Subclasses as necessary based on the types of PII and PHI that were compromised.

93. Representative Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

94. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed classes is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Classes are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiff is informed and believe and, on that basis, allege that the total number of Class Members is in the hundreds of thousands of individuals. Membership in the classes will be determined by analysis of Defendant's records.

b. Commonality: Representative Plaintiffs and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

1) Whether Defendant had a legal duty to Representative Plaintiff and the Classes to exercise due care in collecting, storing, using, and/or safeguarding their PII and PHI;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

6) Whether Defendant adequately, promptly, and accurately informed Representative Plaintiff and Class Members that their PIIand PHI had been compromised;

7) How and when Defendant actually learned of the Data Breach;

8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII and PHI of Representative Plaintiffs and Class Members;

9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Representative Plaintiffs and Class Members;

11) Whether Representative Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;

12) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Representative Plaintiffs' claims are typical of the claims of the Plaintiff Classes. Representative Plaintiffs and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Representative Plaintiffs in this class action are adequate representatives of each of the Plaintiff Classes in that the Representative Plaintiffs have the same interest in the litigation of this case as the Class Members, are committed to vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in its entirety. Representative Plaintiffs anticipate no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Classes to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Classes, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

95. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety. Defendant's

policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Representative Plaintiffs.

96. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII, PHI, and/or financial information of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

97. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

71. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

72. Wing Financial owed a duty to Plaintiffs and all other Class Members to exercise reasonable care in safeguarding and protecting their PII and PHI in its possession, custody, or control.

73. Wing Financial knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class Members' PII and PHI and the importance of maintaining secure systems. Wing Financial knew, or should have known, of the vast uptick in data breaches in recent years. Accordingly, Wing Financial had a duty to protect PII and PHI.

74. Given the nature of Wing Financial's business, the sensitivity and value of the PII and PHI it maintains, and the resources at its disposal, Wing Financial should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring. Wing Financial had a duty to prevent and protect against the unauthorized disclosure of PII and PHI.

75. Wing Financial breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII and PHI entrusted to it—including Plaintiffs' and Class Members' PII and PHI.

76. It was reasonably foreseeable to Wing Financial that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class Members' PII and PHI to unauthorized individuals.

77. But for Wing Financial's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class Members, their PII and PHI would not have been compromised.

78. As a result of Wing Financial's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled

to compensation; (ii) improper disclosure of their PII and PHI; (iii) breach of the confidentiality of their PII and PHI; (iv) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; (vi) fear and anxiety of the impending risk of identity theft; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE PER SE

79. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

80. Wing Financial's duties arise from, in part due to its storage of certain medical information, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

81. Wing Financial's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Wing Financial, of failing to employ reasonable measures to protect and secure PII.

82. Wing Financial's duties further arise from the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1302(d), *et seq.*

83. Wing Financial is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

84. Wing Financial violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. Wing Financial's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

85. Wing Financial's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

86. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

87. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

88. It was reasonably foreseeable to Wing Financial that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

89. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Wing Financial's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for

protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; (vi) fear and anxiety of impending identity theft; and (vii) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY

90. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

91. Plaintiffs and Class Members either directly or indirectly gave Wing Financial their PII and PHI in confidence, believing that Wing Financial – a financial services company – would protect that information. Plaintiffs and Class Members would not have provided Wing Financial with this information had they known it would not be adequately protected. Wing Financial's acceptance and storage of Plaintiffs' and Class Members' PII and PHI created a fiduciary relationship between Wing Financial and Plaintiffs and Class members. In light of this relationship, Wing Financial must act primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiffs' and Class members' PII and PHI.

92. Wing Financial has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard the PII/PHI of Plaintiffs and Class members it collected.

93. As a direct and proximate result of Wing Financial's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII and PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII and PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII and PHI which remains in Wing Financial's possession; (vi) fear and anxiety of the continued risk; and (vii) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (viii) actual or attempted fraud.

COUNT IV
UNJUST ENRICHMENT

94. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein. This claim is pled in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d).

95. Plaintiff and Class Members conferred a monetary benefit upon Wing Financial in the form of monies paid for financial services, healthcare services or other services.

96. Wing Financial accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Wing Financial also benefitted from the receipt of Plaintiffs' and Class Members' PII and PHI.

97. As a result of Wing Financial's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members

paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

98. Wing Financial should not be permitted to retain the money belonging to Plaintiffs and Class Members because Wing Financial failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

99. Wing Financial should be compelled to provide for the benefit of Plaintiffs and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
BREACH OF IMPLIED CONTRACT

100. Plaintiffs reallege and incorporate by reference all allegations of the preceding factual allegations as though fully set forth herein.

101. Defendant required Plaintiffs and Class Members to provide, or authorize the transfer of, their PII and PHI in order for Wing Financial to provide services. In exchange, Defendant entered into implied contracts with Plaintiffs and Class Members in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiffs' and Class Members' PII and PHI and to timely notify them in the event of a data breach.

102. Plaintiffs and Class Members would not have provided their PII and PHI to Defendant had they known that Defendant would not safeguard their PII and PHI, as promised, or provide timely notice of a data breach.

103. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

104. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII and PHI and by failing to provide them with timely and accurate notice of the Data Breach.

105. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members.

COUNT VI
VIOLATION OF THE
OKLAHOMA CONSUMER PROTECTION ACT
15 Okla. Stat. Ann. § 751, *et. seq.*
(On Behalf of the Oklahoma Subclass)

106. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

107. Plaintiffs bring this cause of action individually and on behalf of the members of the Oklahoma Subclass.

108. The Oklahoma Consumer Protection Act was created to protect Oklahoma consumers from unfair methods of competition and unfair or deceptive business practices.

109. Plaintiff and the Oklahoma Subclass contracted with Wing Financial for financial services. As part of their transaction, Wing Financial collected and stored PII/PHI.

110. Wing Financial has its principal place of business and headquarters in Oklahoma, and otherwise engaged in trade or commerce, or conducted business, in Oklahoma.

111. As set forth more fully above, Wing Financial collected consumers' PII/PHI as a part of their doing business. While selling and profiting from its services, Wing Financial failed to adequately maintain safeguards to protect individuals' PII/PHI. Wing Financial concealed this material information from consumers because to do otherwise would have resulted in consumers

seeking other businesses or Wing Financial's competitors for the same services by virtue of Wing Financial's data security policies.

112. Wing Financial's conduct constituted, among other things, the following prohibited fraudulent, deceptive, and unfair business practices: (a) misrepresenting that Wing Financial's data security policy has characteristics, ingredients, uses, or benefits, which it does not have; and (b) engaging in fraudulent and deceptive conduct that creates a likelihood of confusion and misunderstanding.

113. Wing Financial's conduct was fraudulent and deceptive because the omissions created a likelihood of confusion and misunderstanding and had the capacity or tendency to deceive and, in fact, did deceive, ordinary consumers, including Oklahoma Plaintiffs. Ordinary consumers, including Oklahoma Plaintiffs, would have found it material to their choice in services to know that Wing Financial's data security policies were inadequate and that Wing Financial would be collecting PII/PHI that was at serious risk of unauthorized access. Knowledge of those facts would have been a substantial factor in Oklahoma Plaintiffs', as well as Oklahoma Subclass members', decision to contract with Wing Financial.

114. Wing Financial's conduct actually and proximately caused an ascertainable loss of money or property to Oklahoma Plaintiffs (as set forth above) and members of the Oklahoma Subclass. Absent Wing Financial's unfair, deceptive, and/or fraudulent conduct, Oklahoma Plaintiffs and Oklahoma Subclass members would have behaved differently and would not have contracted with Wing Financial. Wing Financial's omissions induced Oklahoma Plaintiffs and Oklahoma Subclass members to contract for services with Wing Financial that they would have otherwise used another entity for.

115. Accordingly, pursuant to the aforementioned statutes, Oklahoma Plaintiffs and Oklahoma Subclass members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence. Those damages are: time and expenses related to monitoring their financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of their personal information, and other economic and non-economic harm. In addition, given the nature of Wing Financial's conduct, Oklahoma Plaintiffs and Oklahoma Subclass members are entitled to recover all available statutory, exemplary, treble, and/or punitive damages, costs of suit, and attorneys' fees based on the amount of time reasonable expended and equitable relief necessary, and all such other relief as the Court deems proper.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiffs, on behalf of themselves and each member of the proposed National Class and the Oklahoma Subclass, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiffs' counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court order Defendant to cease and desist from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiffs' and Class Members' PII and PHI, and from refusing to issue prompt, complete, any accurate disclosures to Representative Plaintiffs and Class Members;

5. For injunctive relief requested by Representative Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiffs and Class Members, including but not limited to an Order:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

c. requiring Defendant to delete and purge the PII and PHI of Representative Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiffs and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiffs' and Class Members' PII and PHI;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

f. prohibiting Defendant from maintaining Representative Plaintiffs' and Class Members' PII and PHI on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Representative Plaintiffs and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiffs, individually, and on behalf of the Class(es) and/or Subclass(es), hereby demand a trial by jury for all issues triable by jury.

Dated: March 17, 2023

FEDERMAN & SHERWOOD

By: /s/ William B. Federman

William B. Federman, OBA # 2853
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
T: (405) 235-1560
F: (405) 239-2112
wbf@federmanlaw.com

SHUB LAW FIRM LLC

/s/ Benjamin F. Johns
Benjamin F. Johns
134 Kings Hwy E., Fl. 2,
Haddonfield, NJ 08033
T: (856) 772-7200
F: (856) 210-9088
jshub@shublawyers.com
bjohns@shublawyers.com

COLE & VAN NOTE

/s/ Laura Grace Van Note
Laura Grace Van Note, Esq. (C.A. S.B. #310160)
555 12th Street, Suite 1725
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: lvn@colevannote.com

Interim Co-Lead Counsel for Plaintiffs